# Department of Homeland Security Daily Open Source Infrastructure Report for 31 July 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

**Daily Highlights**

- The Department of Homeland Security has announced a Notice of Proposed Rulemaking to expand processing in the US−VISIT program −− which records biometric and biographic information to verify the identities of foreign visitors −− to an additional number of non−U.S. citizens. (See item 17)
- The Daily Press reports in Hampton Roads, Virginia, there is a new emergency microwave network linking first responders without using the telephone, Internet, radio, or television. (See item 30)
- CNN reports Seattle police are protecting temples and mosques after a suspected hate killing at the Jewish Federation building in Seattle on Friday, July 28, prompted fears of the Middle East crisis spreading to the United States. (See item 39)



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 28, CanWest News Service* — **Fewer rigs drilling for gas.** Soft natural gas prices are lowering expectations for well numbers, but drilling rigs are staying busy as the industry switches to targets requiring more work. A new forecast Thursday, July 27, by the Petroleum

Services Association of Canada (PSAC) predicted a 7.5 percent drop in total Western Canadian wells to 23,410 this year from 25,290 in 2005. It would be the first decrease since 2002, which was also a year of shaky gas prices. But 596 drilling rigs were working this week, just up from 594 a year ago. About four−fifths of Western Canadian industry activity is in Alberta. The dip is concentrated in fast, shallow gas drilling including coalbed methane programs that respond rapidly to energy market fluctuations, PSAC said.
Source: http://www.canada.com/topics/news/national/story.html?id=3371c515−85b6−41b8−bad2−e072bbf83f69&k=36885

2. *July 28, Bloomberg* — **Gas soars in the heat.** Natural gas soared in New York after a U.S. report showed supplies fell for the first time ever in summer after hot weather last week drove power demand for the fuel. Inventories dropped by seven billion cubic feet, leaving total stockpiles at 2.756 trillion cubic feet last week, and cutting the supply surplus versus the five−year average to 22 percent from 26 percent a week ago.
Source: http://www.thestandard.com.hk/news_detail.asp?we_cat=10&art_id=23829&sid=9052041&con_type=1&d_str=20060728

3. *July 28, Associated Press* — **State opens utilities investigation following St. Louis storm.** State regulators launched an investigation Thursday, July 27, into the way Ameren Corp. and other utilities prepared for and responded to severe storms that left hundreds of thousands of people without electricity. The Missouri Public Service Commission said it had received complaints that Ameren's call center and Internet site could not handle the crush of concerned customers after the first of two storms hit July 19. Investigators also will look into whether Ameren properly kept trees trimmed back from power lines before the storm, how it prioritized its response to downed lines, and how quickly it reached out for help from other utilities. The parameters of the investigation were drawn broadly to also include any other utility whose actions may have affected storm recovery efforts, specifically citing telecommunications company AT&T Inc. and Missouri American Water Co. PSC staff already had begun looking into Ameren's storm preparations and response, which it does routinely after major power outages. By opening a formal investigation, the commission highlighted the importance of the case and provided a way for big electricity consumers such as businesses and local governments to become involved. It set an August 27 deadline for the investigation report.
Source: http://www.newstribune.com/articles/2006/07/28/news_state/15 6state31ameren.txt

4. *July 27, Associated Press* — **Blackout hits London commercial district.** Blackouts caused by sweltering temperatures struck more than 3,000 businesses in London's major shopping district and part of its transit network on Thursday, July 27, officials said. High energy demand led to outages starting in the city's central Soho district, said James Barber of energy company EDF. Barber said the outages were due to a "highly unusual sequence of faults" at substations and in underground cables. Temperatures on Thursday reached 86 degrees in central London. Part of the Oxford Circus subway station, which serves more than 300 nearby stores, was closed for around an hour and a half, causing severe disruption, said James Simpson, a spokesperson for the London Underground. He said an estimated 570,000 passengers ride through the station on weekdays.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/27/AR2006072700868.html

5. *July 27, Nuclear Regulatory Commission* — **NRC proposes $65,000 find for violation at Seabrook station.** The Nuclear Regulatory Commission (NRC) has proposed to fine FPL Energy Seabrook, LLC, $65,000 for a violation related to security requirements at Seabrook Station in Seabrook, NH. The issues were corrected immediately and the plant remains secure. In Spring 2005, the NRC dispatched a special inspection team to Seabrook after a routine security inspection found issues at the site in May. The NRC has cited the company for the failure to maintain complete and accurate records of test results and proposed a $65,000 fine. A second violation that occurred, in part due to inadequate management oversight, has been characterized by the NRC's Reactor Oversight Process as low−to−moderate security significance. NRC Region I Administrator Samuel J. Collins said, "The action was necessary to emphasize the importance of oversight and corporate support of the installation and testing of equipment, as well as maintaining complete and accurate records of such testing."
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 43i.html

6. *July 24, Associated Press* — **Law steps up coalmine safeguards.** Illinois coalmines have new safety standards under a bill signed Sunday, July 23, by Governor Rod Blagojevich (D). The legislation was proposed in response to the Sago Mine disaster in West Virginia that killed 12 miners in early January. The measure requires mine operators to build rescue chambers in Illinois' 18 underground mines to protect employees against potential hazards during an emergency. The chambers would contain first aid materials, oxygen tanks and other materials. The bill calls for each miner to carry portable emergency oxygen tanks, which would need to be checked daily. A stock of the tanks, checked every 90 days, would be located throughout the mine, too.
Source: http://www.suntimes.com/output/news/cst−nws−mines24.html

[Return to top]

## Chemical Industry and Hazardous Materials Sector

7. *July 28, Journal News (OH)* — **Overturned tanker spills fuel, prompts roadway closure.** Authorities Friday morning, July 28, closed a section of Ohio Route 122 between Red Lion and Route 48 after a tanker truck overturned in Warren County, OH, spilling diesel fuel. Drivers were redirected to Route 73 and Route 63 as alternate routes to Interstates 71 and 75.
Source: http://www.journal−news.com/news/content/news/stories/2006/07/28/ws072806tankerspillweb.html?cxtype=rss&cxsvc=7&cxcat=6

[Return to top]

## Defense Industrial Base Sector

8. *July 28, Government Accountability Office* — **GAO−06−793: Defense Technologies: DoD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions (Report).** Major acquisitions in the Department of Defense's (DoD) force transformation rely on maintaining technological superiority to ensure U.S. military dominance. Failure to identify and protect critical technologies makes U.S. military assets vulnerable to cloning, neutralization, or other action that degrades current and anticipated capabilities. To help

minimize these risks, DoD's Militarily Critical Technologies Program developed and periodically updates two lists of technologies −− the Militarily Critical Technologies List (MCTL) and the Developing Science and Technologies List (DSTL). While the lists are primarily intended to inform U.S. export control decisions, they can also inform counterintelligence activities, research plans, and technology protection programs, making MCTL and DSTL fundamental resources for security decisions. To ensure these lists are informative, the Government Accountability Office (GAO) assessed the Militarily Critical Technologies Program's process for updating the MCTL and DSTL and determined how the lists are used to inform export control and DoD policy decisions. GAO is recommending that DoD take several actions to better ensure that efforts to identify critical technologies meet user requirements. DoD concurred with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06793high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−793

[Return to top]

## Banking and Finance Sector

9. *July 30, Finextra* — **Man Group to acquire 70 percent stake in Eurex U.S.** British hedge fund manager Man Group is buying a 70 percent stake in Eurex U.S., the struggling electronic futures market launched in Chicago in 2004, for $23.2 million in cash. Eurex is co−owned by Deutsche Börse and the SWX Swiss Stock Exchange. Deutsche Börse says Man Group will acquire a majority stake in the business and also make a capital injection of $35 million into the exchange, which has been re−named U.S. Futures Exchange (USFE). Eurex launched its U.S. exchange in February 2004 to compete against the Chicago Board of Trade (CBOT) and Chicago Mercantile Exchange (CME) in U.S. Treasury futures trading. But the unit has failed to capture a significant share of the market and has struggled since its launch. The venture will now aim at providing new products for hedge funds and retail investors, rather than compete against the established futures exchanges in Chicago.
Source: http://finextra.com/fullstory.asp?id=15649

10. *July 27, Federal Financial Institutions Examination Council* — **FFIEC releases updated information security booklet.** The Federal Financial Institutions Examination Council (FFIEC) Thursday, July 27, issued revised guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions. The Information Security Booklet is one of twelve that, in total, comprise the FFIEC IT Examination Handbook. In addition to the revised Information Security Booklet, the agencies also released an Executive Summary that contains high level synopses of each of the twelve booklets and describes the handbook development and maintenance processes. The Information Security Booklet describes how an institution should protect and secure the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers (TSPs) to maintain effective security programs tailored to the complexity of their operations.
Information Security Booklet and Executive Summary: http://www.ffiec.gov/guides.htm
Source: http://www.ffiec.gov/press/pr072706.htm

11. *July 27, TechWeb* — **eBay, PayPal users hit hardest by phishing.** Three out of every four phishing attacks target users of online auctioneer eBay and its electronic payment system PayPal, Sophos said Thursday, July 27. Of the phishing e−mails captured so far in 2006 by Sophos' network of spam traps 54.3 percent took aim at PayPal users and 20.9 percent tried to dupe users of eBay. Graham Cluley of Sophos said, "Although bank customers do also suffer from phishing attacks, they tend to be less likely to have the global reach that these net giants have." Sophos' numbers differ from the Anti−Phishing Working Group, of which the security company is a member. According to the APWG's most recent data, 92 percent of phishing attacks in May were directed at brands and companies in the financial services sector. That number hasn't changed significantly since the start of 2006.
Source: http://www.techweb.com/wire/security/191501877;jsessionid=C2ZWVZH40P3YWQSNDLPCKH0CJUNN2JVN

12. *July 27, Websense Security Labs* — **Multiple Phishing Alert: BNP Paribas, CashU Card, Central Bank of the Republic of Turkey, Wescom Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of BNP Paribas. Users are given a link to a fraudulent Website where they are prompted to enter their account and personal information. Another new phishing attack targets customers of CashU Card. Users receive a spoofed e−mail message claiming that their account has been limited as a result of unusual activity. The e−mail message contains a link to a phishing Website, which attempts to capture the account password, address, and credit card information. A new phishing attack targets customers of the Central Bank of the Republic of Turkey. Users are sent a spoofed e−mail with a link to a fraudulent website where they are prompted to enter their account and personal information. Another new phishing attack targets customers of Wescom Credit Union. Users receive a spoofed e−mail message, which claims that multiple computers have accessed their account, and they need to change their password or their account will be deactivated. The message provides a link to a phishing Website that requests users to log on and provide account details to keep their accounts active.
Screenshots: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =561
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =562
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =563
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =564
Source: http://www.websensesecuritylabs.com

[Return to top]

## Transportation and Border Security Sector

13. *July 29, Associated Press* — **Virtual view clears sky for pilots.** Near−blind landings in foul weather may soon be a lot less perilous, thanks to new corporate jet equipment that could also find its way into airliner cockpits. The technology, known as Synthetic Vision Systems (SVS), displays a computer−generated view of the terrain ahead −− even in heavy fog or clouds, when the ground can be invisible to other advanced "vision" equipment such as infrared sensors. Gulfstream Aerospace became the first executive plane maker to announce plans to offer an SVS aboard its jets. The deal was announced at last week's Farnborough Air Show in the UK. The equipment is a highly detailed, three−dimensional Global Positioning System (GPS) satellite navigation screen for planes. Existing satellite navigation systems already allow pilots

to pinpoint their positions. The SVS display uses the same GPS satellite signals to show a pilot exactly where the plane is heading −− in enough detail to carry out landing approaches or other precision maneuvers in low visibility. Instead of the traditional blue−over−brown artificial horizon, a pilot using the new screen sees an ever−changing virtual view from the cockpit, overlaid with the familiar altitude, attitude, speed, and heading indicators.
Source: http://www.usatoday.com/travel/flights/2006−07−28−virtual−co ckpit_x.htm

14. *July 29, Boston Globe* — **Federal transportation official urges full review of Big Dig project.** A top federal transportation official is raising concerns about the adequacy of the state's Big Dig safety review, saying it should examine “the entire project,” including ramps, roadways, and area bridges. Todd J. Zinser, the Department of Transportation's acting inspector general (IG), sent a letter late Thursday, July 27, to members of Massachusetts’ state congressional delegation expressing concern that the “safety audit of all tunnels” ordered by the Legislature could overlook important items. He cited the need to test ramps, roadways, and Boston's bridges, in addition to the underground portions of the Big Dig. He also said that tests are necessary on mechanical and electrical systems, such as ventilation and fire−control equipment, as well as security procedures and emergency−response communications. The inspector general is examining the overall management of the $14.6−billion project. In his letter, Zinser wrote that the additional federal money would help expand “investigative, audit, and engineering units,” and bring in outside experts from the Army Corps of Engineers. The inspector general described his role as that of oversight over the various state and federal agencies that are conducting investigations.
IG Central Artery Tunnel/Project letter: http://www.oig.dot.gov/item.jsp?id=1854
Source: http://www.boston.com/news/traffic/bigdig/articles/2006/07/2 9/us_urges_full_review_of_big_dig/

15. *July 28, Source: Government Accountability Office* — **GAO−06−869: Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened (Report).** The Transportation Security Administration (TSA) is responsible for screening all checked baggage in U.S. airports for explosives and has deployed explosive detection systems and developed standard procedures for their use. TSA also allows alternative screening procedures to be used for short−term, special circumstances. This report addresses (1) how TSA prioritized the use of checked baggage screening procedures and identified trade−offs in security effectiveness and operational efficiencies; (2) how TSA reported use of the procedures and ensured that standard procedures are used whenever possible; and (3) what steps TSA took to reduce airports’ need to use alternative screening procedures and to establish performance measures to monitor their use. To address these issues, the Government Accountability Office (GAO) interviewed TSA officials, reviewed information from TSA’s database on checked baggage screening operations; and conducted airport site visits. GAO is recommending that TSA use information on airport usage of alternative screening procedures in conducting covert testing; strengthen TSA’s monitoring and tracking of the use of alternative screening procedures; and develop performance measures and targets for the use of alternative screening procedures. DHS reviewed a draft of this report and generally concurred with GAO’s findings and recommendations.
Highlights: http://www.gao.gov/highlights/d06869high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−869

16. *July 27, Government Accountability Office* — **GAO−06−823: Information Technology: Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses but Key Improvements Still Needed (Report).** The Department of Homeland Security's (DHS) fiscal year 2005 appropriations act provided $39.6 million for Immigration and Customs Enforcement's (ICE) program to modernize its information technology (IT) infrastructure. The goals of the program −−which consists of seven projects and is referred to as Atlas −− include improving information sharing and strengthening security. As mandated by the appropriations act, the department is to develop and submit for approval an expenditure plan for Atlas that satisfies certain legislative conditions, including a review by the Government Accountability Office (GAO). In performing its review of the Atlas plan, GAO was asked to (1) determine whether the plan satisfies certain legislative conditions, (2) determine the status of our prior recommendations, and (3) provide any other observations about the plan and management of the program. GAO is recommending that DHS minimize Atlas program risks by, among other things, developing and implementing project plans consistent with elements of effective project planning. DHS did not provide additional substantive comments on this report recognizing that ICE had already agreed with the briefing contained in this report.
Highlights: http://www.gao.gov/highlights/d06823high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−823

17. *July 27, Department of Homeland Security* — **Department of Homeland Security proposes expansion of visitors enrolled in US−VISIT.** The Department of Homeland Security (DHS) announced on Thursday, July 27, a rule proposing to expand processing in the US−VISIT program to an additional number of non−U.S. citizens. A Notice of Proposed Rulemaking was published in the Federal Register. A final rule will establish an effective date. US−VISIT records biometric and biographic information to verify the identities of foreign visitors to the United States. Most visitors experience US−VISIT biometric collection procedures −− digital, inkless finger scans and digital photograph −− upon entry to the United States and at visa−issuing posts around the world. Expanding the population processed through US−VISIT is the next step in a plan to improve public safety and national security, as well as ensure the integrity of the immigration process. It is consistent with a number of initiatives that strengthen the integrity of travel documents issued to foreign visitors seeking entry into the United States, as it verifies the travel documents' holder by their biometrics. US−VISIT currently applies to all foreign visitors (with limited exemptions) entering the United States, whether they are traveling on a visa or by air, sea, or land. This includes foreign visitors traveling under the Visa Waiver Program. Foreign visitors under age 14 and over age 79 are exempt from US−VISIT procedures.
Source: http://www.dhs.gov/dhspublic/display?content=5762

18. *July 20, Transportation Security Administration* — **TSA announces new background check requirement for Hazmat drivers licensed in Canada or Mexico.** The Transportation Security Administration (TSA) has announced that beginning August 10, 2006 drivers licensed in Canada or Mexico to commercially transport hazardous materials will be required to undergo a background check under the Bureau of Customs and Border Protection's (CBP) Free and Secure Trade (FAST) program before transporting placarded amounts of hazardous materials (Hazmat) in the United States. The Safe, Accountable, Flexible, Efficient Transportation Equity Act: a Legacy for Users (SAFETEALU) requires that, beginning August 10, 2006, commercial

drivers licensed in Canada or Mexico may not transport Hazmat, including explosives, within the U.S. unless they have undergone a background check similar to that required for U.S. operators with a Hazmat endorsement. The FAST program is a cooperative effort among the CBP and the governments of Canada and Mexico to coordinate processes for the clearance of commercial shipments at the border. Northern and southern border FAST driver cards are valid at any CBP land border crossing where the technology currently exists.
Information on the application process may be found on the CBP Website:
http://www.cbp.gov/xp/cgov/import/communications_to_trade/ad vance_info/
For more information see the Hazmat Threat Assessment Program Website:
http://www.tsa.gov/what_we_do/layers/hazmat/editorial_multi_ image_with_table_0219.shtm
or call (877) 429−7746.
Source: http://www.tsa.gov/press/releases/2006/press_release_0725200 6.shtm

19. *June 28, Government Accountability Office* — **GAO−06−554: Highway Finance: States' Expanding Use of Tolling Illustrates Diverse Challenges and Strategies (Report).** Congestion is increasing rapidly across the nation and freight traffic is expected to almost double in 20 years. In many places, decision makers cannot simply build their way out of congestion, and traditional revenue sources may not be sustainable. As the baby boom generation retires and the costs of federal entitlement programs rise, sustained, large−scale increases in federal highway grants seem unlikely. To provide the robust growth that many transportation advocates believe is required to meet the nation’s mobility needs, state and local decision makers in virtually all states are seeking alternative funding approaches. Tolling (charging a fee for the use of a highway facility) provides a set of approaches that are increasingly receiving closer attention and consideration. This report examines tolling from a number of perspectives, namely: (1) the promise of tolling to enhance mobility and finance highway transportation, (2) the extent to which tolling is being used and the reasons states are using or not using this approach, (3) the challenges states face in implementing tolling, and (4) strategies that can be used to help states address tolling challenges. The Government Accountability Office (GAO) is not making any recommendations. GAO provided a draft of this report to U.S. Department of Transportation (DOT) officials for comment.
Highlights: http://www.gao.gov/highlights/d06554high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−554

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

20. *July 28, Agence France−Presse* — **China reports new foot−and−mouth outbreak.** China has reported a fresh outbreak of foot−and−mouth disease, with 54 head of cattle affected in the nation's northwestern Qinghai province. Cattle at a farm in Qinghai's Haixi Mongolian region began showing symptoms of the illness last week and they were diagnosed with

foot−and−mouth disease on Thursday, July 27. A total of 98 cattle were culled following the outbreak, while local agriculture officials quarantined and disinfected the farms and the surrounding area. There have been at least three other outbreaks in Qinghai this year of foot−and−mouth disease, a severe and highly contagious viral disease affecting cattle, pigs, sheep and other livestock.
Source: http://news.yahoo.com/s/afp/20060728/hl_afp/healthchinafarm_060728131045;_ylt=AiqP.6IsjLV1mLXXczcrNCmJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**21.** *July 28, AgProfessional* — **Years of drought show farmers, ranchers need to be prepared.** Several years of drought across Nebraska have shown farmers and ranchers that the best time to develop a successful drought management plan is before drought strikes. To deal with drought, producers are reducing cattle numbers, practicing better grazing management and doing a host of other related practices, a year of surveys and interviews conducted by the National Drought Mitigation Center revealed. The surveys and interviews found that producers dealing best with the drought had drought management plans in place before the drought began, said Cody Knutson, water resources scientist with the National Drought Mitigation Center. Surveys were mailed to Nebraska members of the former Holistic Resource Management group, Sustainable Agricultural Society and Organic Crop Improvement Association. In addition, 47 producers were interviewed across the state, including farmers, ranchers and organic producers.
Source: http://www.agprofessional.com/show_story.php?id=42197

**22.** *July 28, Associated Press* — **Experts seek cause of death for local ducks.** The North Carolina Department of Agriculture still doesn't know exactly what killed several ducks and left others sick earlier this week in downtown Swansboro. But it's definitely not bird flu, state officials said Thursday, July 27. Representatives from the Department of Agriculture were in Swansboro Wednesday, July 26, collecting samples from sick Moscovy ducks. A necropsy was also done on one of the dead birds, but the cause of death isn't known yet, said Brian Long, spokesperson for the Department of Agriculture. Officials are running a variety of tests −− everything from toxicology to bacterial tests −− in an attempt to rule things out.
Source: http://www.jdnews.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=43626&Section=News

[Return to top]

## Food Sector

Nothing to report.
[Return to top]

## Water Sector

**23.** *July 27, NBC 17 (NC)* — **Wells tainted by dry cleaner condemned.** Chemicals left behind years ago by a defunct dry cleaner have contaminated several private drinking wells in Raleigh, NC. Solvents used by Pro Cleaners, which operated in what is now the Towne North Plaza shopping center before closing in the 1970s, have seeped into the groundwater and are

spreading, state environmental officials said. Although the chemicals remain within recommended limits, the levels are rising, officials said. "The contamination from dry cleaners can travel 1,000, 2,000 feet away from their source," said John Powers, of the state Department of Environment and Natural Resources. "It can just be so small, but if it's continuous over a long period of time, it can add up."
Source: http://www.nbc17.com/health/9587551/detail.html

[Return to top]

## Public Health Sector

**24.** *July 30, Agence France−Presse* — **India plans new polio immunization drive after 136 cases reported.** India has launched an immunization drive targeting 45 million children after recording 136 cases of polio since January, an official said. What was alarming was the reappearance of polio in Jharkhand and Madhya Pradesh, two states that had previously eliminated the virus. The vaccination drive starts Sunday, July 30. India accounted for 83 percent of the world's new polio cases in 2002 with 1,600 cases recorded that year. In India the number of cases was cut to 66 in 2005.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://news.yahoo.com/s/afp/20060730/hl_afp/healthpolioindia_060730100438;_ylt=AnaXVC79wqxQMSfOdWiKBIuJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**25.** *July 30, Reuters* — **New bird flu outbreak along Thai−Lao border.** The H5N1 bird flu virus has been found in the Thai northeast bordering Laos, prompting culling of 310,000 hens after the virus killed a teenager elsewhere in the country last week, the Agriculture Ministry said on Sunday, July 30. "The lab results confirmed last night chickens from a village in Nakohn Panom province have died of bird flu," Vice Agriculture Minister Charal Trinwuthipong said. "The culling on all 78 farms has already begun and we hope to finish them all by Sunday night," he said. Charal said the outbreak in Nakohn Panom, 460 miles northeast of Bangkok, might be caused by H5N1−infected egg trays taken from "the other side" of the border, in an apparent reference to Laos. A 17−year−old man died of bird flu on Monday, July 24, in the northern province of Phichit, where authorities have slaughtered hundreds of birds and restricted poultry movement in a bid to stamp out Thailand's first outbreak in eight months.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=worldNews&storyID=2006−07−30T072237Z_01_BKK78049_RTRUKOC_0_UK−BIRDFLU−THAILAND.xml&archived=False

**26.** *July 29, Associated Press* — **People fall ill aboard cruise ship in Caribbean.** Nearly 230 people aboard a cruise ship fell ill with a gastrointestinal illness during a weeklong Caribbean voyage, the cruise line said Saturday, July 29. The illness, believed to be a norovirus brought onto the Mariner of the Seas by a passenger, struck 221 of the ship's 3,660 passengers and six of its 1,202 crewmembers, said Royal Caribbean spokesperson Michael Sheehan. Sick passengers started complaining of vomiting and diarrhea Wednesday, July 26, and were treated with over−the−counter medication, he said. This is the second outbreak aboard the Mariner of the Seas this year. In January, the ship reported a norovirus that sickened 276 passengers and 27 crew members.

Source: http://www.orlandosentinel.com/news/local/state/orl−bk−cruiseill2906jul20,0,5296071.story?track=rss

**27.** *July 29, Associated Press* — **Rabbit fever returns to Martha's Vineyard.** Massachusetts public health officials are warning people on Martha's Vineyard about the dangers of a potentially fatal disease known as "rabbit fever" after six new cases were identified. Cases of the disease tularemia, or rabbit fever, have occurred on Martha's Vineyard every year since an initial outbreak in 2000 sickened 15 people and resulted in one fatality, according to the Department of Public Health. More than three−dozen confirmed cases have been reported on the island in the last five years. Those affected on Martha's Vineyard range in age from 33 to 67 and became ill between May 13 and July 5. All six, four of whom are employed as landscapers, have been treated and are recovering, officials said. All of the cases reported this year had the respiratory form of the disease. Tularemia information: http://www.cdc.gov/ncidod/diseases/submenus/sub_tularemia.ht m
Source: http://www.foxnews.com/wires/2006Jul29/0,4670,RabbitFever,00 .html

**28.** *July 28, Associated Press* — **Post−Katrina, hospitals still struggling.** You go to the drugstore to refill a prescription and learn the doctor's left town. You spend an extra week in pain because disk surgery isn't an emergency. You're admitted to a hospital, but the rooms are full, so you spend days in the ER. That's what it's like in New Orleans if you need health care. The system is in serious condition, 11 months after Hurricane Katrina. Within the next two to three months, "all the hospitals" will be considering cutting services, said Mark Peters, board chairman of the Metropolitan Hospital Council of New Orleans. Since the chaotic days after the storm and the subsequent flooding, hundreds of doctors have fled the city, says Gery Barry, chief executive for Blue Cross and Blue Shield of Louisiana, one of the state's largest insurers. "About three−quarters of the physicians who'd been practicing in the New Orleans area are no longer submitting claims to us," he said.
Source: http://www.chron.com/disp/story.mpl/ap/nation/4080074.html

**29.** *July 28, Agence France−Presse* — **Bird flu found on poultry farm in Laos.** An outbreak of the H5N1 strain of bird flu has killed more than 2,000 chickens on a poultry farm in Laos, the government and Food and Agriculture Organization (FAO) said. Veterinarians had slaughtered 6,000 more birds on the farm about 15 miles south of the national capital, disinfected the cages and declared a three−mile surveillance zone, they said. The Xaythani district farm, which previously suffered a bird flu outbreak in early 2004, found 155 dead chickens on July 14, and about 2,000 dead birds the following day, said the FAO chief technical advisor on avian influenza in Laos, Ricarda Mondry. Samples were then sent to a laboratory, where tests confirmed that the chicken had died of the H5N1 strain, she said. In May Laos found the H5N1 virus in a single duck in a backyard farm near the capital Vientiane, but extensive testing in villages in following months had found no further cases.
Source: http://news.yahoo.com/s/afp/20060728/wl_asia_afp/healthflulaos_060728093234;_ylt=Atjb77ncQT708P.BuS5lzZSJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

# Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

**30.** *July 29, Daily Press (VA)* — **Microwave network links first responders in Virginia.** In Hampton Roads, VA, there is a new emergency microwave network that can operate without the phone, Internet, radio, or television. The wireless network has been in the works for about three years. It connects the Emergency Operations Centers for 16 cities and counties in Hampton Roads, allowing them to better communicate in case of a natural disaster or terrorist strike. In addition to providing a secure phone line, it allows for videoconferencing and electronic file−sharing among local jurisdictions. Although the system is operational, most personnel haven't been trained on it yet, and it hasn't been used in an actual emergency.
Source: http://www.dailypress.com/news/local/dp−83892sy0jul29,0,390734.story?coll=dp−news−local−final

**31.** *July 28, KHNL−TV (HI)* — **Emergency communications exercise held at Aloha Stadium in Hawaii.** In Honolulu, HI, police, fire and other emergency response agencies worked on tuning their radios together Friday, July 28 during a training exercise at Aloha Stadium. "We want to make sure if this thing happens we want to be able to communicate across the board," said Honolulu Mayor Mufi Hannemann. In many cities, police, firefighters and medical teams use incompatible radio systems, leaving them unable to communicate. Organizers declared the exercise a success but say there's room for improvement.
Source: http://www.khnl.com/Global/story.asp?S=5213249

[Return to top]

## Information Technology and Telecommunications Sector

**32.** *July 28, IDG News Service* — **Google to host repository for open−source projects.** Google is offering to host open source software development projects in a move that has been met with mixed reaction from the developer community online. As part of the new offering, launched on Thursday, July 27, developers get 100MB of disk space to store and share their open source project, and can use tools such as issue tracking and mailing list support. Google said it is making the offer in an effort to encourage healthy, productive open source communities. Developers must have a Gmail account to use the service.
Project Hosting on Google Code: http://code.google.com/hosting/
Project Hosting Frequently Asked Questions: http://code.google.com/hosting/faq.html
Source: http://www.infoworld.com/article/06/07/28/HNgoogleopensource_1.html

**33.** *July 28, Agence France−Presse* — **Asia Pacific countries hatch plan to thwart cyber attacks.** The Associations of Southeast Asian Nations Regional Forum is expected to announce sweeping plans to prevent cyber attacks on critical infrastructure and the abuse of online resources by terrorists. Countries will pledge to share intelligence, expertise and skills on fighting cyber crime, and look at laws to prevent terrorist attacks being planned or encouraged

through computer networks. The nations will also make efforts to draw up cyber crime and cyber security laws and implement national frameworks to address criminal and terrorist uses of online networks.
Source: http://news.yahoo.com/s/afp/20060728/tc_afp/aseanarfattacksinternet;_ylt=Ag7HfvWZR.Q3.Jn6bGYr3jAjtBAF

**34.** *July 28, Government Accountability Office* — **GAO−06−863T: Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan (Testimony).** Since the early 1990s, growth in the use of the Internet has revolutionized the way that our nation communicates and conducts business. While the Internet originated as a U.S. government−sponsored research project, the vast majority of its infrastructure is currently owned and operated by the private sector. Federal policy recognizes the need to prepare for debilitating Internet disruptions and tasks the Department of Homeland Security (DHS) with developing an integrated public/private plan for Internet recovery. The Government Accountability Office (GAO) was asked to summarize its report being released Friday, July 28 −− Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan, GAO−06−672 (Washington, DC: June 16, 2006). This report (1) identifies examples of major disruptions to the Internet, (2) identifies the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluates DHS plans for facilitating recovery from Internet disruptions, and (4) assesses challenges to such efforts. In its report, GAO suggests that Congress consider clarifying the legal framework guiding Internet recovery and makes recommendations to DHS to strengthen its ability to help recover from Internet disruptions. In written comments, DHS agreed with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06863thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−863T

**35.** *July 27, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−208A: Mozilla products contain multiple vulnerabilities.** The Mozilla Web browser and derived products contain several vulnerabilities, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system.
Systems Affected: Mozilla SeaMonkey; Mozilla Firefox; Mozilla Thunderbird. Any products based on Mozilla components, specifically Gecko, may also be affected.
To view vulnerability details: http://www.kb.cert.org/vuls/byid?searchview&query=firefox_1505
Solution: Upgrade to Mozilla Firefox 1.5.0.5, Mozilla Thunderbird 1.5.0.5, or SeaMonkey 1.0.3.
Firefox 1.5.0.5: http://www.mozilla.com/firefox/
Thunderbird 1.5.0.5: http://www.mozilla.com/thunderbird/releases/1.5.0.5.html
SeaMonkey 1.0.3: http://www.mozilla.org/projects/seamonkey/ In addition, these vulnerabilities can be mitigated by disabling JavaScript and Java in all affected products. Instructions for disabling Java in Firefox can be found in the "Securing Your Web Browser" document: http://www.us−cert.gov/reading_room/securing_browser/#ffcont ent
Source: http://www.uscert.gov/cas/techalerts/TA06−208A.html

**36.** *July 27, Security Focus* — **Microsoft Internet Explorer NDFXArtEffects stack overflow vulnerability.** Microsoft Internet Explorer is prone to a stack overflow vulnerability. Analysis: A stack overflow can occur by setting one of the RGBExtraColor, RGBForeColor, and

RGBBackColor properties to a long string value. Since the entire string is placed into a stack buffer, you are able to select exactly what instruction to fault on based on the length of the string to cause the system to crash.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/19184/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/19184/references

**37.** *July 27, Reuters* — **Nokia starts tests of Wi−Fi Internet mobile calls.** Nokia has started its first tests in Oulu, Finland, of a technology that allows users to roam seamlessly between phone networks and local wireless hotspots such as Wi−Fi. Mobile subscribers with handsets enabled for so−called unlicensed mobile access, or UMA, can make calls over the Internet when they are in range of an unlicensed wireless network such as Bluetooth or Wi−Fi. When they move out of range, the connection will automatically revert to a GSM, GPRS or UMTS mobile phone network.
Source: http://www.eweek.com/article2/0,1895,1995163,00.asp

**38.** *June 16, Government Accountability Office* — **GAO−06−672: Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan (Report).** Since the early 1990s, growth in the use of the Internet has revolutionized the way that our nation communicates and conducts business. While the Internet was originally developed by the Department of Defense, the vast majority of its infrastructure is currently owned and operated by the private sector. Federal policy recognizes the need to prepare for debilitating Internet disruptions and tasks the Department of Homeland Security (DHS) with developing an integrated public/private plan for Internet recovery. The Government Accountability Office (GAO) was asked to (1) identify examples of major disruptions to the Internet, (2) identify the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluate DHS plans for facilitating recovery from Internet disruptions, and (4) assess challenges to such efforts. GAO is suggesting that Congress consider clarifying the legal framework guiding Internet recovery. GAO is also making recommendations to the Secretary of the Department of Homeland Security to strengthen the department’s ability to serve as a focal point for helping to recover from Internet disruptions by completing key plans and activities and addressing challenges. In written comments, DHS agreed with GAO’s recommendations.
Highlights: http://www.gao.gov/highlights/d06672high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−672

## Internet Alert Dashboard

**DHS/US−CERT Watch Synopsis**

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** US−CERT has received information that a website on the Internet is hosting malicious software that has been or is currently being used to compromise systems.

**IP:** 211.34.248.244

**Activity:**
This activity is similar to what was reported on July 6th concerning the "beststartmotor" domain. The original email stated: "In April 2006, users reported having their web browsers redirected from other websites to the domain beststartmotor.com using an HTML command called an iframe. Once redirected, the victim's web browsers usually download malware onto the victim's computer." Currently, another website may have a similar iframe link to IP 211.34.248.244. Once a web browser on a victim system follows this link, the victim computer may download malware which can compromise that computer.

**Recommendation:**
US−CERT suggests that each agency evaluate the potential risk and take protective measures in a manner that is consistent with the agency's policies and procedures. Please refrain from investigating / visiting the IP address as this may result in accidental infection of your computer. Please be advised that the IP address listed above may also host additional domains and websites. However, this information is being shared to allow the GFIRST community to understand the potential risk associated with those domains.

US−CERT requests that all agencies examine firewall, web proxy and other network perimeter device logs for suspicious traffic to and from the above IP. Should you encounter such activity, please notify US−CERT at soc@us−cert.gov or via phone at 888−282−0870.

**Active Exploitation of a Vulnerability in Microsoft PowerPoint**
US−CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

**VU#936945:** Microsoft PowerPoint contains an unspecified remote code execution vulnerability. http://www.kb.cert.org/vuls/id/936945

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments. http://www.us−cert.gov/cas/tips/ST04−010.html

US−CERT will continue to update current activity as more information becomes available.

**PHISHING SCAMS**

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 44139 (−−−), 1026 (win−rpc), 4672 (eMule), 27164 (−−−), 445 (microsoft−ds), 25 (smtp), 24232 (−−−), 6881 (bittorrent), 80 (www), 6346 (gnutella−svc)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

**39.** *July 29, CNN* — **Seattle protects temples, mosques after "hate" shootings.** Seattle police were protecting temples and mosques Saturday, July 29, after a suspected hate killing prompted fears of the Middle East crisis spreading to the United States. Police Chief Gil Kerlikowske said a Muslim gunman killed a woman and wounded five others at the Jewish Federation building in Seattle, WA, Friday afternoon, July 28, and police were protecting mosques as well as synagogues out of fears of retaliation. A U.S. citizen, Naveed Afzal Haq, has been arrested and booked on a charge of murder and five charges of attempted murder. The 31−year−old Muslim of Pakistani descent was angry at Israeli airstrikes in Lebanon, officials said. In a written statement, the Council on American−Islamic Relations on Friday condemned the attack. Robert Jacobs, Regional director for the Jewish Anti−Defamation League, said the group has been warning Jewish institutions to be wary and have adequate security because of the ongoing conflict in the Middle East. Assistant Police Chief Nick Metz said police had no specific information about any threats, but his department had issued an alert on Thursday "reminding officers to be vigilant to monitor synagogues and mosques in the city."
Source: http://www.cnn.com/2006/US/07/29/seattle.shooting/index.html

[Return to top]

# General Sector

**40.** *July 29, CNN* — **Hundreds flee Nebraska fire.** At least 900 residents evacuated Chadron, in western Nebraska, after wildfires reached the town's border and caught several houses on fire Saturday, July 29, Nebraska Emergency Management Agency spokesperson Jim Bunstock said.

Firefighters worked early Saturday to control six wildfires burning since late Wednesday after multiple lightning strikes hit dry grasslands in the northwestern area of the state, Bunstock said. The wildfires span across a 25−mile area, he said. Personnel from the state and federal National Guard, federal firefighters, and other agencies are assisting in quelling the fire, which may grow or shift given Saturday's "hot, windy and dry" forecasted weather conditions, Bunstock said. Further evacuations depend on the damage produced by the two fires that were burning parts of Chadron late Friday into Saturday.
Source: http://www.cnn.com/2006/US/07/29/nebraska.fires/index.html

[Return to top]

**DHS Daily Open Source Infrastructure Report Contact Information**

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

**DHS Daily Open Source Infrastructure Report Contact Information**

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

**Department of Homeland Security Disclaimer**